Please type a plus sign (+) inside this box [+]

PTO/SB/05 (1/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

Only for new nonprovisional applications under 37 C.F.R. 1.53(b)

Attorney Docket No.	NTL-3.2.076/2120 (BAO-418)
First Inventor or Application Identifier	Tal Lavian
Title	Security Association Mediator For Java-Enabled Devices
Express Mail Label No.	EL284834038US

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [x] *Fee Transmittal Form (e.g., PTO/SB/17)
(submit an original, and a duplicate for fee processing)

2. [x] Specification Total Pages [11]
(preferred arrangement set forth below)

- Descriptive title of the invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R&D
- Reference to Microfiche Appendix
- Background of the invention
- Brief Summary of the invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. [X] Drawing(s) (35 U.S.C. 113) Total Pages [2]

4. Oath or Declaration Total Pages [2]
a. [x] unexecuted (original or copy)
b. [ ] Copy from a prior application (37 CFR §1.63(d)
(for continuation/divisional with box 16 completed)
i. [ ] DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R.§ 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.26).

5. [ ] Microfiche Computer Program (Appendix)

6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. [ ] Computer Readable Copy
b. [ ] Paper Copy (identical to computer copy)
c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [ ] Assignment Papers (cover sheet & document(s))

8. [ ] 37 C.F.R. §3.73(b) Statement [ ] Power of Attorney
(when there is an assignee)

9. [ ] English Translation Document (if applicable)

10. [X] Information Disclosure Statement (IDS)PTO-1449 [X] Copies of IDS Citations

11. [ ] Preliminary Amendment

12. [X] Return Receipt Postcard (MPEP 503)
(should be specifically itemized)

13. [ ] *Small Entity [ ] Statement filed in prior application
Statement(s) (PTO/SB/09-12) Status still proper and desired

14. [ ] Certified Copy of Priority Document(s)
(if foreign priority is claimed)

15. [X] Other: Check No. For $ 760.00

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No.: /

Prior application information: Examiner _____ Group/Art Unit: _____

For CONTINUATION or DIVISIONAL APPS. Only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered to be part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label (Insert Customer No. Or Attach bar code label here) or [X] Correspondence address below

Name	COBRIN & GITTES				
Address	750 Lexington Avenue, 21 floor				
City	New York	State	New York	Zip Code	10022
Country	U.S.A.	Telephone	(212) 486-4000	Fax	(212) 486-4007

Name (Print/Type)	Ricahrd M. Lehrer	Registration No. (Attorney/Agent)	58,356
Signature	Richard M Lehrer	Date	May 7, 1999

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231.

EXPRESS MAIL CERTIFICATE

Date: May 7, 1999 Label No EL284834038US
I hereby certify that, on the date indicated above I deposited this paper or fee with the U S Postal Service and that it was addressed for delivery to Box Patent Application, the Assistant Commissioner for Patents, Washington, DC 20231 by "Express Mail Post Office to Addressee" service.

Lucretia Husain Lucretia Husain
Name (Print) Signature

APPLICATION
FOR
UNITED STATES LETTERS PATENT

TO ALL WHOM IT MAY CONCERN:

Be it known that Tal Lavian, Franco Travostino, Thomas Hardjono and Robert Duncan have invented a SECURITY ASSOCIATION MEDIATOR FOR JAVA-ENABLED DEVICES of which the following description in connection with the accompanying drawings is a specification, like reference characters on the drawings indicating like parts in the several Figures.

SECURITY ASSOCIATION MEDIATOR FOR JAVA-ENABLED DEVICES

FIELD OF THE INVENTION

This invention relates generally to the field of networking and more particularly to methods and apparatus for transferring files between devices in a secure manner.

BACKGROUND OF THE INVENTION

Data networks have become an essential part of most businesses. With the advent and wide acceptance of the Internet they have become even more essential.

Many network systems, such as telephone network products, data network products, etc. include externally developed software applications that call various functions within the network. It is desirable, however, to limit the functions and/or information that can be called by the application or the visitor to those that are necessary and/or approved.

It is thus important for a business to take precautions against downloading a code which may be potentially damaging to its network (e.g. a code which accesses the internal resources of a switch or router, such as the routing tables or filtering information, etc) and to take precautions against unauthorized access by outsiders.

It is unlikely that computers which access the Internet will ever be completely safe from attack from hackers and viruses. However, systems are available which provide a level of protection and security against such problems.

The Java environment includes security devices such as a security manager, a byte code verifier and a class loader. A security manager is a local device which determines whether potentially threatening or unauthorized operations should be allowed. A byte code verifier verifies the byte code transmitted with the download, and the class loader loads the Java Byte code to the JVM.

However, the security devices of a respective environment may not be backward compatible with earlier versions. In the Java environment, as an example, the security devices in version 1.2 are not backward compatible with those in versions 1.1 and 1.0.2, and the security devices in version 1.1 are not backwards compatible with those in version 1.0.2. Thus, an application program written in a respective version of Java is not compatible with other versions.

Furthermore, in some programming environments, such as in the Java environment, the security devices provide multi-level security but are not transparent, namely the user code must explicitly interact with the system, and the security devices are not dynamic, namely that off-line changes to the system may be necessary. Alternatively, the security devices are code transparent but do not provide multi-level security.

Accordingly, there exists a need for a security system which is system wide which prevents harmful programs from being downloaded onto a network.

There exists a need for a security system which is system wide and which prevents unauthorized access to the internal resources of a switch or router.

There also exists a need for such a system which enables a system view or configuration.

There also exists the need for such a system which is distributed.

There exists a need for such a system which allows other security entities to participate in the security system.

Accordingly, it is an object of the present invention to provide a security system which prevents harmful programs from being downloaded onto a network.

It is an object of the invention to provide a security system which prevents unauthorized access to the internal resources of a switch or router.

It is another object of the invention to provide such a system which is system wide and which enables a system view or configuration.

It is still another object of the invention to provide such a system which is distributed.

It is another object of the invention to provide a such a system which allows other security entities to participate in the security.

These and other objects of the invention will become apparent to those skilled in the art from the following description thereof.

SUMMARY OF THE INVENTION

In accordance with the teachings of the present invention, these and other objects may be accomplished by the present invention, which provides a method for providing security against unauthorized access to internal resources of a network device. The method includes receiving a digital signature at a security association manager (SAM) wherein the digital

signature includes an encryption code. The SAM requests a de-encryption code, de-encrypts the digital signature with the de-encryption code, authenticates the de-encrypted digital signature, and requests allowed operations associated with the authenticated signature.

An embodiment of the invention includes apparatus for providing security against unauthorized access to internal resources of a network device. The apparatus includes a security association manager (SAM) configured to receive a digital signature including an encryption code. The SAM is configured to send a message including a portion of the digital signature. The message includes a request for an encryption decoder. The SAM is further configured to receive a response to the message. The SAM is also configured to send a digitally signed message requesting allowed operations associated with the digital signature in response to receiving the reply message.

Another embodiment of the invention includes apparatus for providing security against unauthorized access to internal resources of a network device. The apparatus includes a module for receiving a digital signature including an encryption code. It also includes a module for accessing a de-encryption code in electrical communication with the module for receiving; and, it includes a module for determining allowed operations associated with the digital signature.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be more clearly understood by reference to the following detailed description of an exemplary embodiment in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates a block diagram of a security system in accordance with the present invention.

FIG. 2 illustrates a block diagram of a distributed security system in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention provides a system and method of providing network security while transferring Java code between devices and/or while allowing access to Java enabled devices (e.g., within a network, between devices on a network and the Internet, between devices on separate networks, between network devices and application servers, and/or between network devices and databases.).

As illustrated in Fig. 1, the system provides a Security Association Manager 20 (SAM) which performs, *inter alia*, certain security tasks which are not performed by conventional Java security systems. The SAM 20 is distributed throughout the network and may be part of the class loader 10. Those skilled in the art will recognize that the SAM 20 may be integral with the class loader 10, co-located with, but logically separate from the class loader 10 or entirely distinct therefrom and still fall within the scope of the invention. The SAM 20 may be realized in hardware and/or software. As illustrated in Fig. 1,the system includes conventional class loaders 10, SAMs 20, a certificate authority 30, a policy server 40, access managers 50, security managers 70 and byte code verifier 60. The SAM 20 verifies the authenticity of the entity and either allows a download/access to a device or rejects the download/access to a network device. The certificate authority 30 is a repository for public key certificates and may be a part of the secure network or part of the unsecured network. The policy server 40 is a repository for the rights (privileges) an entity is entitled to on the secure network. The class loader 10 loads the Java Byte Code to the JVM. The Access Manager 50 assigns access levels to each Java thread that is created. The security manager 70 is a conventional security manager and the byte code verifier 60 verifies that the Byte code is valid Java code.

When Java code is to be transferred to a Java enabled network device (JEND) in the secure network, the code is digitally signed. A digital signature is generally a string of bits that is computed from a combination of the data being signed and a private key of an entity. A private key certificate (private key) is generally a number that is supposed to be known only to a particular entity, although it may not even be known to the entity (e.g. it may be associated with that entity through a program that entity employs). Either way, a private key is meant to be kept secret. A private key is always associated with a public key.

A digitally signed Java code is received by the class loader 10 and may be employed by the SAM 20, which is in communication with the class loader 10, to verify that the data came from an authorized entity or with the authority of an authorized entity. A digital signature can be authenticated via a computation that uses the public key corresponding to the private key used to generate the signature. It cannot be forged, assuming the private key is kept secret. It is a function of the data signed and thus can not be claimed to be the signature for other data as well. Further, the signed data cannot be changed; if it is, the signature will no longer authenticate.

The SAM 20 receives the digital signature, reads a name or code which is attached thereto then sends a request (including the name/code which was attached to the digital signature) for the public key certificate to the certificate authority 30. The certificate authority 30 compares the received request to the information stored therein. If no match is found then the certificate authority 30 responds to the SAM 20 with a message indicating failure (e.g., certificate does not exist, etc.). If the certificate authority finds a match, then it returns the public key certificate to the SAM 20.

If the SAM receives the failure notification it rejects the download/denies access. If the SAM receives the public key certificate, it authenticates the digital signature using the public key.

After the SAM 20 authenticates the digital signature, it sends a request for the rights the entity has on the secure network. The request is digitally signed or encrypted and sent to the policy server 40. While in the preferred embodiment the request to the policy server is digitally signed, it is possible to use other forms of security or no security at all if so desired, since the request typically will occur over the secure network and all SAMs could have the same rights to see the requested information. In the preferred embodiment the request is encoded since generally not all SAMs have the same rights on the network. The policy server 40 verifies the authenticity of the request from the SAM 20, then returns the access level stored in the policy server 40 corresponding to the request. The response is also digitally signed or encrypted to prevent it from being modified during transit. However, since this is also traveling over the secured network it is foreseeable that this message could be designed to have no security attached to it. Once the SAM receives this information and authenticates

the transmission, it allows the download of the code/access to the system to take place within the limits of the entity's rights on the network.

The operation of the SAM with respect to providing further access is described in further detail in U.S. Application Serial No. _____, filed concurrently herewith (NTL-3.2.077/2128), which is incorporated herein by reference.

It will thus be seen that the invention efficiently attains the objects set forth above, among those made apparent from the preceding description. In particular, the invention provides methods and apparatus for providing network security against unauthorized access to Java enabled devices. Those skilled in the art will appreciate that the configuration depicted in Figures 1 and 2 provide such features.

It will be understood that changes may be made in the above construction and in the foregoing sequences of operation without departing from the scope of the invention. It is accordingly intended that all matter contained in the above description or shown in the accompanying drawings be interpreted as illustrative rather than in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention as described herein, and all statements of the scope of the invention which, as a matter of language, might be said to fall there between.

Having described the invention, what is claimed as new and secured by Letters Patent is:

1. A method of providing security against unauthorized access to internal resources of a network device comprising:

receiving a digital signature at a security association manager (SAM); wherein said digital signature includes an encryption code;

said SAM requesting a de-encryption code;

said SAM de-encrypting said digital signature with said de-encryption code;

said SAM authenticating said de-encrypted digital signature; and

said SAM requesting allowed operations associated with said authenticated signature.

2. A method of providing security according to Claim 1 wherein said network device comprises a Java enabled device.

3. A method of providing security according to Claim 1 wherein said encryption code comprises a private key and said de-encryption code comprises a public key certificate associated with said private key.

4. A method of providing security according to Claim 1 further comprising:

a certificate authority receiving said request for a de-encryption code and comparing information in said request to information stored in said certificate authority.

5. A method of providing security according to Claim 4 further comprising:

said certificate authority responding to said request by sending said de-encryption code to said SAM.

6. A method of providing security according to Claim 1 further comprising:

a policy server receiving said request for allowed operations associated with said authenticated signature;

said policy server comparing said authenticated signature with information stored on said policy server; and

said policy server sending a response to said SAM indicating an access level corresponding to said authenticated signature.

7. A method of providing security according to Claim 6 further comprising:

said policy server authenticating said request for allowed operations associated with said authenticated signature prior to comparing said authenticated signature with said information stored on said policy server.

8. Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

a security association manager (SAM); configured to receive a digital signature including an encryption code;

wherein said SAM is configured to send a message including a portion of said digital signature; wherein said message includes a request for an encryption decoder;

wherein said SAM is further configured to receive a response to said message;

wherein said SAM is configured to send a digitally signed message requesting allowed operations associated with said digital signature in response to receiving said reply message.

9. Apparatus for supplying security in accordance with Claim 8 further comprising:

a certificate authority configured to receive said message from said SAM, and to send said reply; wherein said certificate authority includes

10. Apparatus for providing security according to Claim 8 wherein said network device comprises a Java enabled device.

11. Apparatus for providing security according to Claim 8 wherein said encryption code comprises a private key and said encryption decoder comprises a public key certificate associated with said private key.

12. Apparatus for providing security according to Claim 8 further comprising:

a policy server configured to receive said request for allowed operations associated with said authenticated signature;

said policy server including a comparison device configured to compare said authenticated signature with information stored on said policy server; and

said policy server being configured to send a response to said SAM indicating an access level corresponding to said authenticated signature.

13.Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

means for receiving a digital signature including an encryption code;

means for accessing a de-encryption code in electrical communication with said means for receiving; and,

means for determining allowed operations associated with said digital signature.

14. Apparatus for providing security according to Claim 13 wherein said network device comprises a Java enabled device.

15. Apparatus for providing security according to Claim 13 further comprising a downloadable file associated with said digital signature.

16. Apparatus for providing security according to Claim 13 wherein said encryption code comprises a private key.

17.Apparatus for providing security according to Claim 13 wherein said de-encryption code comprises a public key certificate.

18. Apparatus for providing security according to Claim 13 further comprising means for receiving a downloadable filing including said digital signal and assigning an access level to a java thread.

ABSTRACT

The invention provides a system and method for providing security against unauthorized access to a java enabled network device. The system includes multiple conventional class loaders, code verifiers, security managers, access managers, SAMs, a certificate authority and a policy server. The SAM verifies the authenticity of the entity and either allows a download/access to a device or rejects the download/access to a network device. The certificate authority is a repository for public key certificates and may be a part of the secure network or part of the unsecured network. The policy server is a repository for the rights (privileges) an entity is entitled to on the secure network. The code verifiers verify that the Byte Code is valid java code. The security manager is the conventional security manager. The class loader loads the code to the device and the access manager assigns access levels to each Java thread that is created.

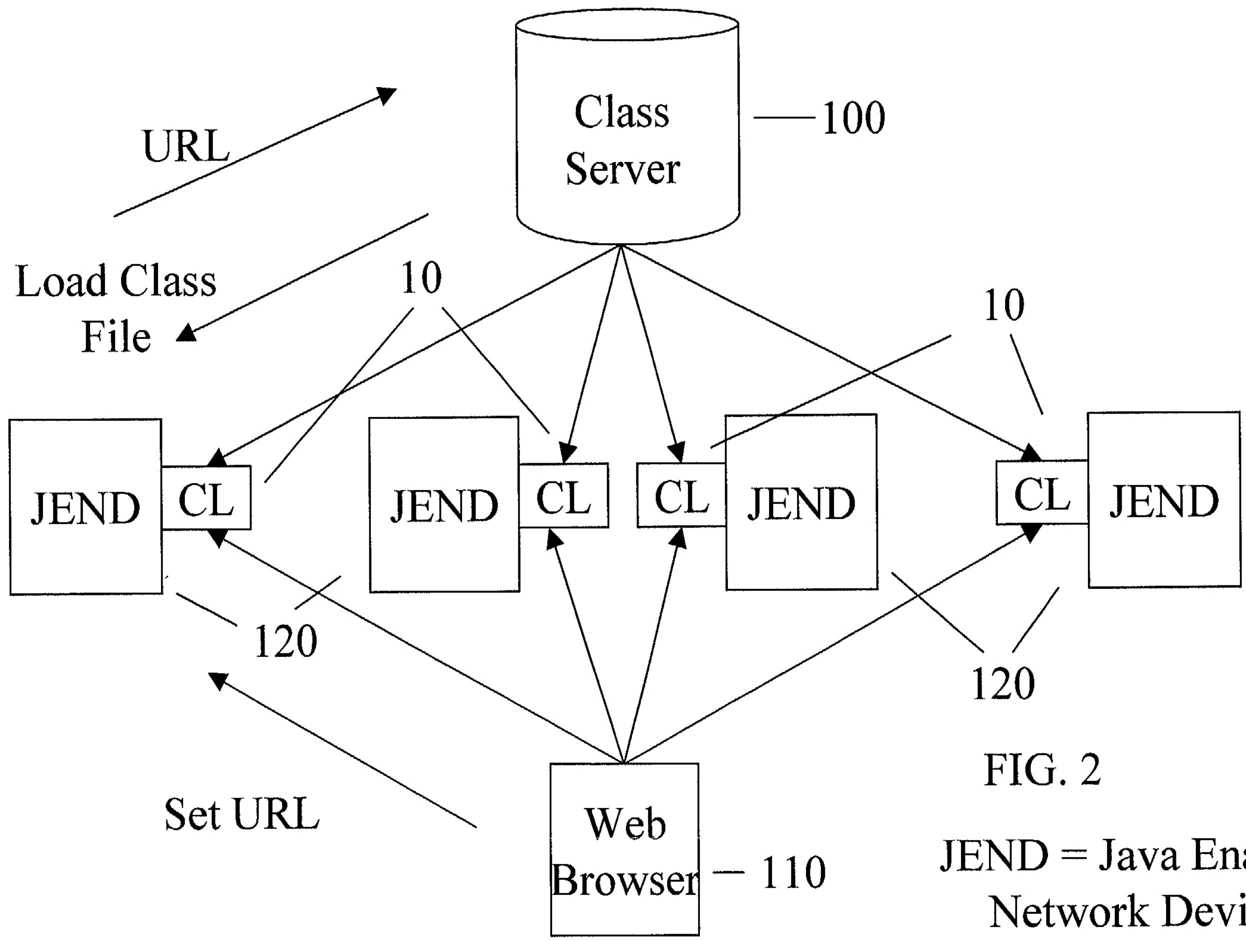

FIG. 2

JEND = Java Enabled Network Device
CL = Class Loader

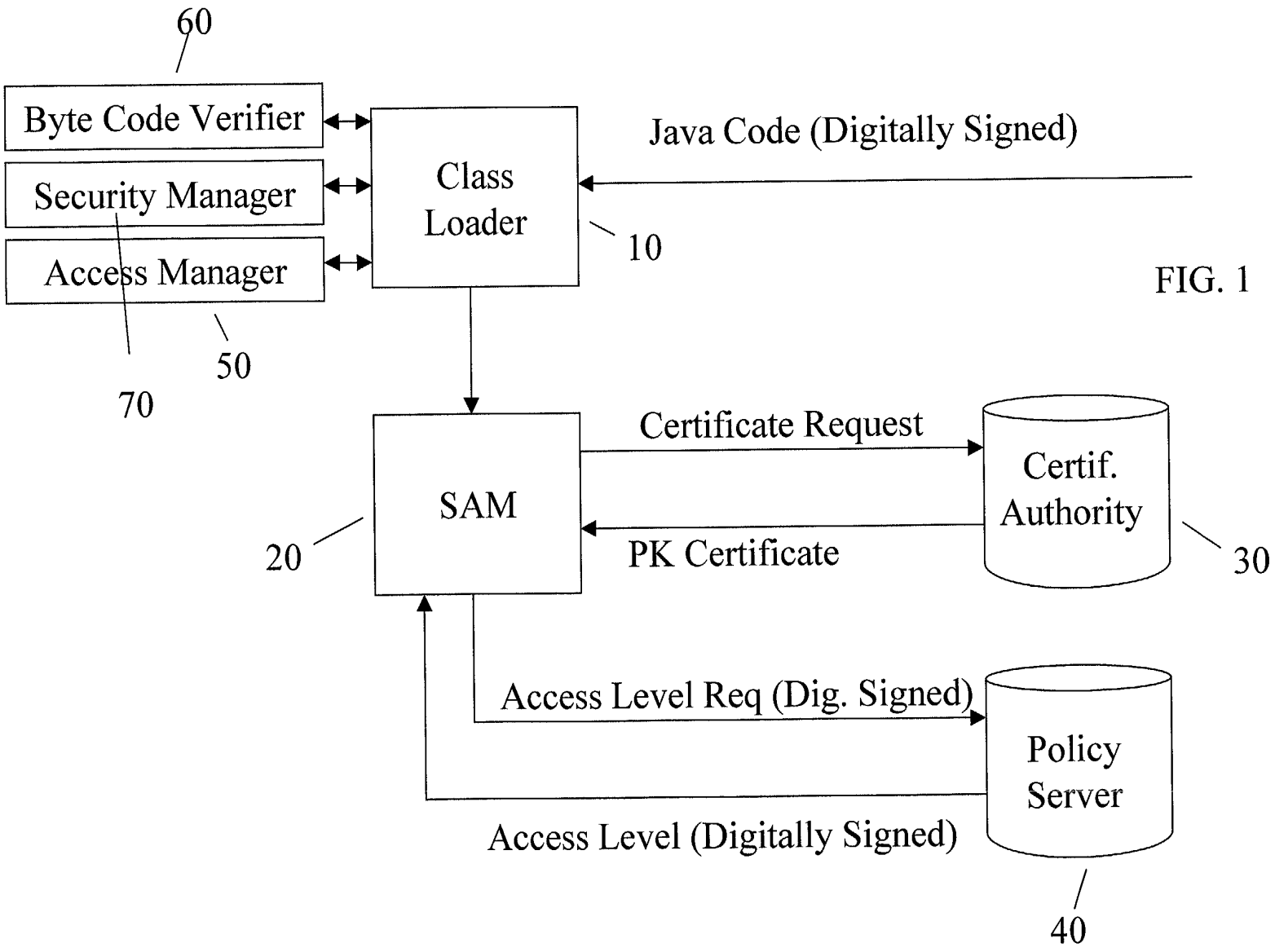

FIG. 1

Attorney Docket No.: NTL-3.2.076/2120 (BAO-418)

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURITY ASSOCIATION MEDIATOR FOR JAVA-ENABLED DEVICES

specification of which is attached hereto unless the following is checked:

[ ] was filed on _____ as United States Application Number or PCT International Application Number _____
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.
I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s).			Priority Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	__ Yes __ No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	__ Yes __ No

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

_____ (Application Number)	_____ (Filing Date)
_____ (Application Number)	_____ (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1 56 which became available between the filing date of the prior application and the national or PCT International filing date of this application

_____ (Application Number)	_____ (Filing Date)	_____ (Status - patented. pending, abandoned)
_____ (Application Number)	_____ (Filing Date)	_____ (Status - patented, pending, abandoned)

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: Peter T Cobrin, Reg No. 24,117, Marvin S. Gittes, Reg. No 24,350, Richard M. Lehrer, Reg. No. 38,536, Robert J. Hess, Reg. No. 32,139, David W. Denenberg, Reg. No 40,986, Michael A. Adler, Reg No. 38,810, Gerald J. Cechony, Reg. No. 31,335, Lawrence E. Russ, Reg. No. 35,342.

Address all correspondence to. COBRIN & GITTES
750 Lexington Avenue, New York, New York 10022 Telephone· (212) 486-4000 Facsimile. (212) 486-4007

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true: and further that these statements were made with the knowledge that willful false statement and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor (given name, family name) Tal Lavian
Inventor's signature _____ Date: _____
Residence: Sunnyvale, California
Post Office Address: **1351 Zurich Terrace, Sunnyvale, California 94087**
Citizenship: Israel

Full name of second joint inventor (given name, family name) Franco Travostino
Inventor's signature _____ Date: _____
Residence: Arlington, Massachusetts
Post Office Address: **53 Westmoreland Avenue, Arlington, MA 02174**
Citizenship: Italy

Full name of third inventor (given name, family name) Thomas Hardjono
Inventor's signature _____ Date: _____
Residence: Arlington, Massachusetts
Post Office Address: **10 Fessenden Road, Arlington, MA 02476**
Citizenship: Australia

X Additional inventors are being named on separately numbered sheets attached hereto.

DECLARATION FOR PATENT APPLICATION
PAGE 2 OF 2

Title: SECURITY ASSOCIATION MEDIATOR FOR JAVA-ENABLED DEVICES

Full name of fourth inventor (given name, family name) Rob Duncan
Inventor's signature _____ Date: _____
Residence: San Francisco, California
Post Office Address: **3274 20th Street, San Francisco, California**
Citizenship: United Kingdom

Full name of fifth inventor (given name, family name) _____
Inventor's signature _____ Date: _____
Residence: _____
Post Office Address: _____
Citizenship: _____

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statement and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

____ Additional inventors are being named on separately numbered sheets attached hereto.

F:\WPDATA\NORTEL\2120\DECL&POW.WPD